Contemporary Engineering Sciences, Vol. 9, 2016, no. 22, 1075 - 1083
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2016.66113

Links Failure Analysis of Averaging Executed by Protocol Push–sum

Martin Kenyeres

Dept. of Telecommunications, Brno University of Technology
Technická 12, 612 00 Brno, Czech Republic

Jozef Kenyeres

Sipwise GmbH, Europaring F15, 2345
Brunn am Gebirge, Austria

Vladislav Škorpil

Dept. of Telecommunications, Brno University of Technology
Technická 12, 612 00 Brno, Czech Republic

Abstract

In this paper, we examine the impact of a links failure on the push–sum protocol. This protocol is very suitable for the implementation into WSNs and therefore, we verify the robustness of the unsecured execution of this protocol. Our primary focus is a comparison of the impact of this failure on the push-sum protocol in the strongly and the weakly-connected structures. We focus on a verification of the mass conservation theorems, the impact on the distribution of the convergence rates, the impact on the diversity of the final results, the change of the convergence rates and the deviation of the final results from the expected ones.

Keywords: distribution computing, push–sum protocol, links failure analysis

1 Introduction

The wireless sensor networks (labelled as WSNs) are classified as distributed systems consisting of a set of spatially distributed devices whose main goal is to

measure and process a particular environmental quantity [3]. These devices (labelled as nodes) are characterized by limited computing capabilities and energy sources [3]. Despite these constraints, the WSNs found a usage in various applications [4]. The functionality of these networks is based on a mutual communication of the particular nodes. Usually, the nodes are deployed in a large–scale area within which they measure a particular quantity [3]. So, the mutual communication among the nodes situated in remote geographical areas poses an energy–demanding and complicated process. However, the mutual communication is necessary for a proper functionality because a statistically processed set of data obtained by independent nodes ensures a higher statistical credibility of the observed phenomenon. Therefore, it is required to implement a complementary mechanism ensuring measured data processing into the WSNs.

Due to the mentioned constraints of these networks, the latest research is focused on distributed solutions. One of the appropriate solutions is a gossip–based multifunctional algorithm – the push–sum protocol [1]. Its execution is inspired by spreading information via gossips. The set of the gossip–based protocols poses simple energy–undemanding solutions that are significantly resistant to a potential failure nevertheless [5]. Thus, this aspect is a very important reason of why this protocol is appropriate for an implementation into WSNs.

As mentioned, the push–sum protocol can fulfil multiple functionalities after small modifications. Within this paper, our attention is focused on a calculation of the average of the measured values. In this case, each node is allocated the initial value (which can be the result of a measurement) and the weight, which is set to 1 for all the nodes [1]. At each iteration, each node sends a half of its inner state and a half of its weight to one of its neighbors chosen uniformly at random. The same value is stored in its inner memory. At the end of each iteration, the node calculates the sum of all the inner states sent by the nodes from its adjacent area and from the stored one in the inner memory – the results represents the inner state for the next iteration. The same procedure is repeated for the calculation of the weights. The ratio of these two sums (the sum of the inner states is the numerator) represents the estimation of the average of all the initial values. The nodes communicate only within their adjacent area and slowly converge to the value equaling the average of all the initial values [1].

The rise of this paper was motivated by the lack of the papers verifying the theoretically declared resistance of this protocol.

2 Experiments and discussion

Within this section, our attention is focused on examining the impact of a links failure on the push–sum protocol. We assume that a transmission failure between two nodes is modeled using a Bernoulli distribution. In our case, it means that there is the probability p whose value determines the probability of a link failure. We also assume that a link breakdown stuns only one transmission procedure. We examine the effect of this failure on randomly–generated strongly and weakly–connected topologies (we used the generator from [2]). Their representatives are shown in Fig.

1. In order to ensure more credible conclusions, each set consists of ten randomly generated networks. We assume that the probability of a link failure can take ten values: {0%,10%,20%,30%,40%,50%,60%,70%,80%,90%}. We do not assume the value equaling 100% because the protocol is unable to fulfil its functionality in such a scenario. Furthermore, as the push–sum protocol is a stochastic protocol whose parameters may vary when its execution is repeated, we repeat each experiment 10 000 times. Within this paper, we examine the impact of this failure on the mass conservation theorems, the impact on the distribution of the convergence rates, the impact on the diversity of the final results, the change of the convergence rates and the deviation of the final results from the expected ones.

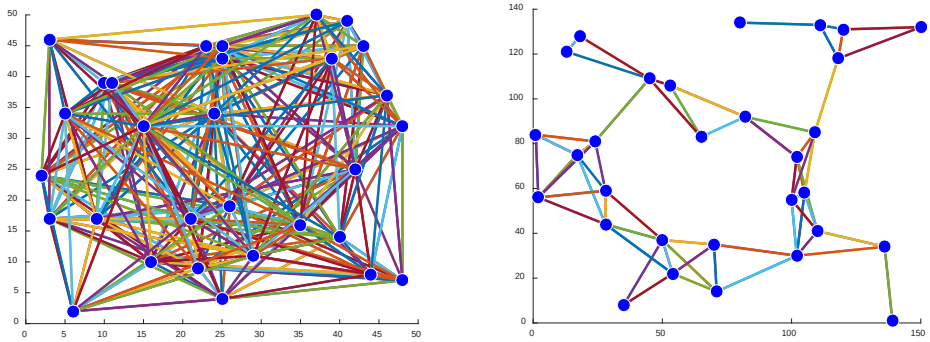

Fig. 1. Representatives of the examined sets

2.1. The impact of a links failure on the mass conservation theorems

The goal of this section is to show the impact of a links failure on the mass conservation theorems. The first theorem says about the constant value of the sum of all the inner values, meanwhile, the second one about the constant value of the sum of all the weights [1]. It is necessary to preserve these theorems to ensure a proper functionality of the push–sum protocol. As we assume that a links failure results in a messages loss, the conservation theorems are not supposed to hold. We examine the change of the value of p on the sum of the inner states and the sum of the weights. In order to ensure the transparency of the depicted results, we show the results for $p = 0$, 0.1, 0.3 and 0.5. We use a color differentiation and the results have been shown for five executions. The character is same also for the other values. We have shown the obtained results in the following sequence of the figures:

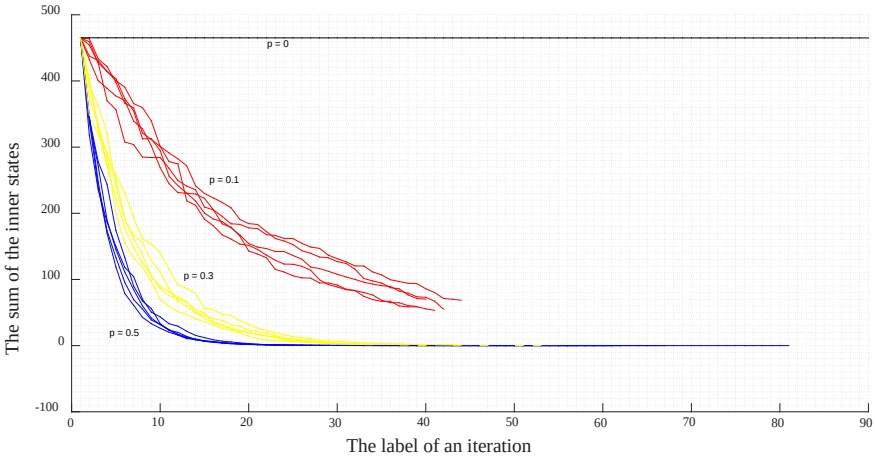

Fig. 2. Mass conservation – theorem 1 – strongly connected structure

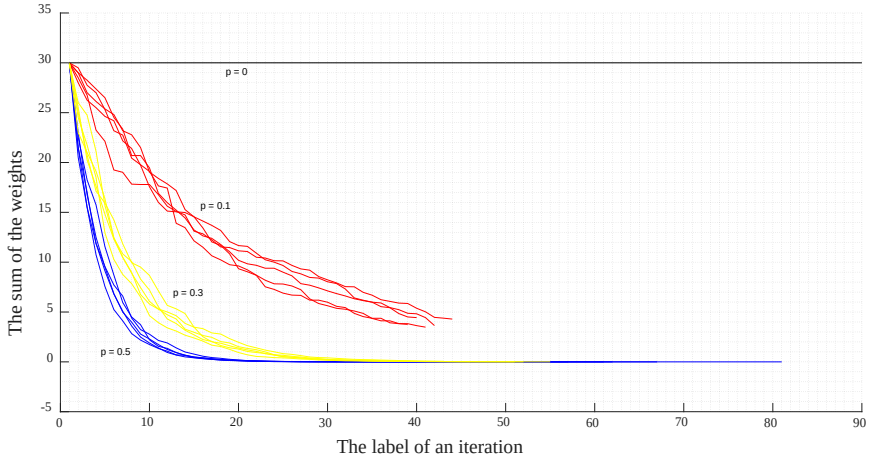

Fig. 3. Mass conservation – theorem 2 – strongly connected structure

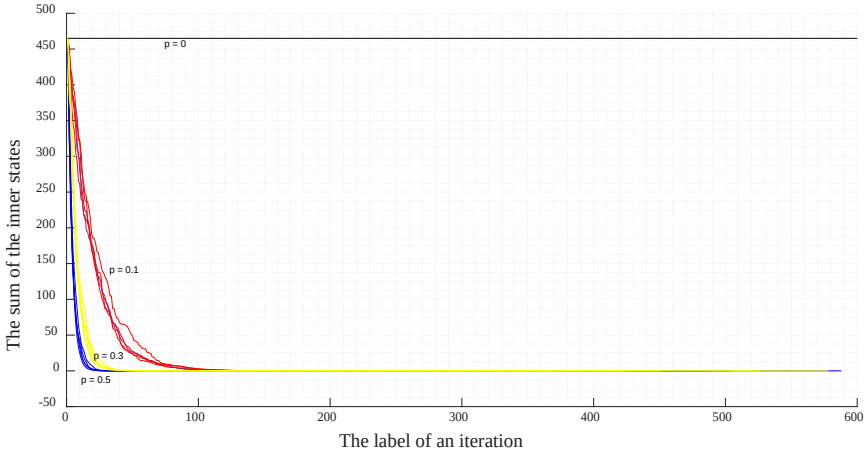

Fig. 4. Mass conservation – theorem 1 – weakly connected structure

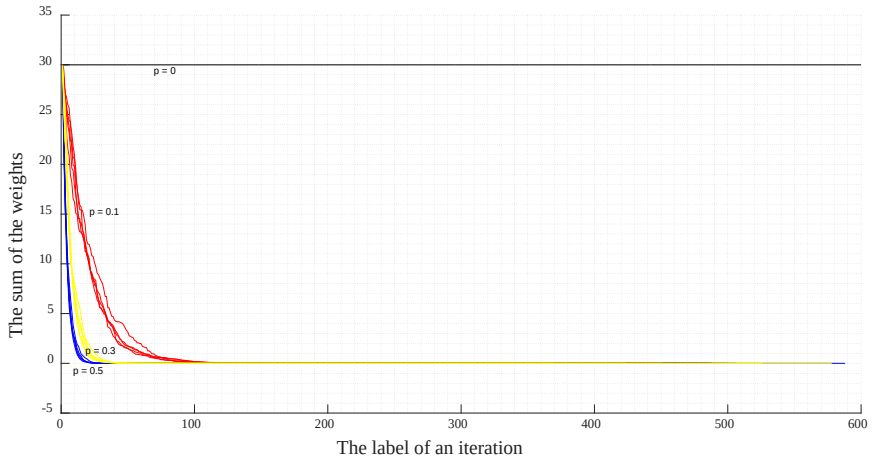

Fig. 5. Mass conservation – theorem 2 – weakly connected structure

We can see from the results that the sum of both parameters decreases more significantly for the higher values of *p*. Thus, we proved the theoretical assumptions that the theorems would not be fulfilled because of lost messages.

2.2. The impact of a links failure on the distribution of the convergence rates

Within the next experiment, we examine the distribution of the achieved convergence rates. As already mentioned, in order to obtain a statistically credible output, each experiment consists of 10 000 executions (the initial conditions are preserved and therefore, the diversity is caused only by a stochastic character of the push–sum protocol). In Fig. 6, we have shown the results obtained in a strongly–connected structure. Again, in order to ensure the transparency of the figure, we have shown only the results for p = 0, 0.3, 0.5 and 0.7.

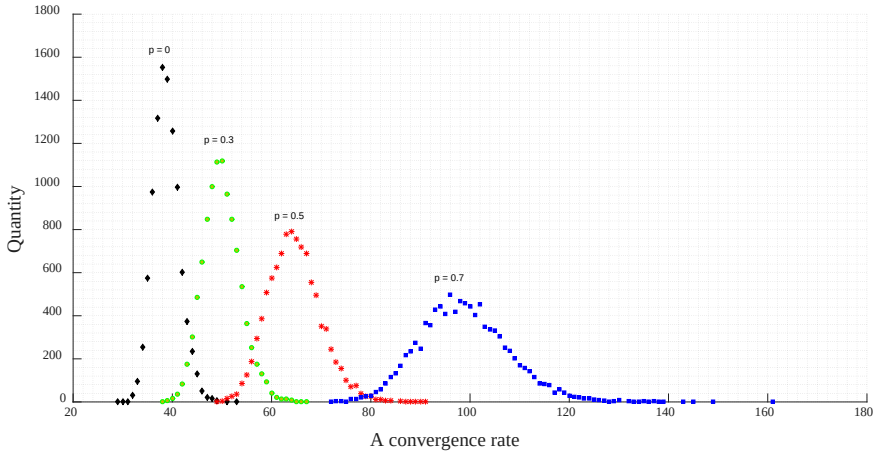

Fig. 6. The distribution of the convergence rates in strongly–connected topologies

We can see from the results that a higher value of p causes a more significant deceleration of the protocol as well as a wider spread of the obtained data. The obtained data can be classified as a data set of a Gaussian distribution.
For the weakly–connected structures, the character of the obtained data differs from the previous case. We observe the interesting phenomenon that a links failure may even accelerate the computation process. We can see from the Fig. 7 that the average convergence rate is smaller for small values of p than in the mistake–free scenario. Then the number of the iterations necessary for the push–sum protocol to be completed starts growing dramatically. The distribution of the data is similar to the previous case, i.e. a higher value of p results in a higher variation (even though the average convergence rate is smaller compared with the mistake–free scenario). However, the mentioned acceleration is not desired phenomenon because the final values to which the nodes converge differ from the real average.

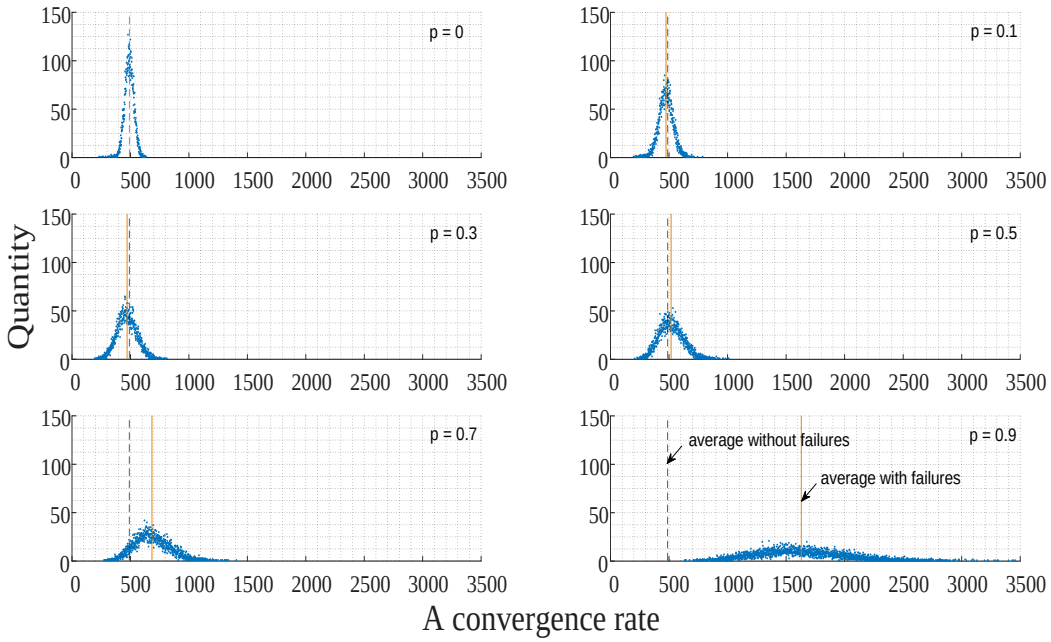

Fig. 7. The distribution of the convergence rates in weakly–connected topologies

2.3. The impact of a links failure on the diversity of the final results

The next experiment is focused on examining the effect of a links failure on the diversity of the final results to which the nodes converge. We show the results for p = 0.1, 0.4, 0.7 and 0.9. We can see from the results that the character of the observed phenomenon is same for both types of the networks. A higher value of p causes the final results to be wider spread. In the weakly–connected structures, the variance is more significant.

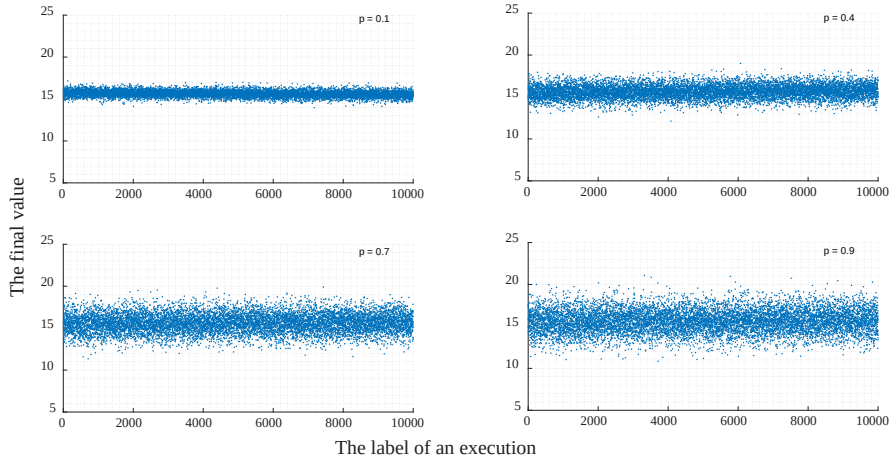

Fig. 8. The diversity of the final results in strongly–connected structure

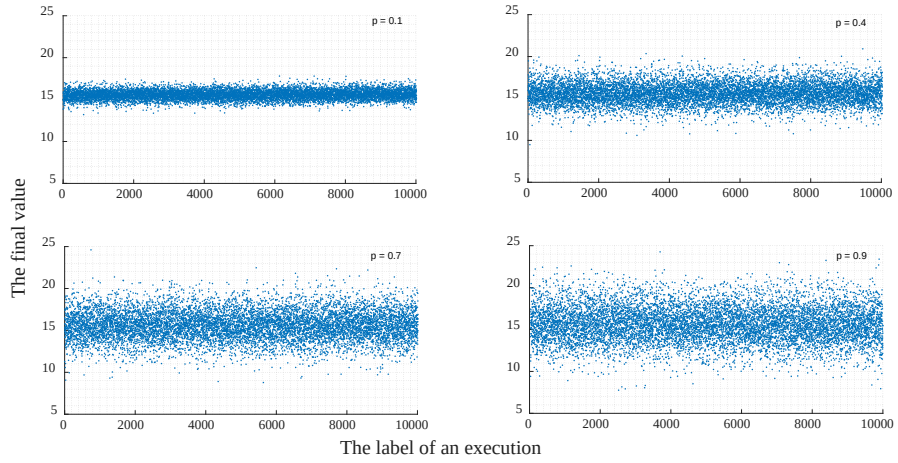

Fig. 9. The diversity of the final results in weakly–connected structure

2.4. The impact of a links failure on the change of the convergence rate and the deviation of the final results from the expected ones

Within the last experiment, we examine the effect of a links failure on the change of the convergence rates and the deviation of the final values from the expected ones. We have repeated the experiment for 20 randomly generated topologies (10 strongly and 10 weakly–connected). The experiment was again repeated 10 000 for each p and each topology. The average value was chosen as a representative of the obtained results. The obtained results have been shown in Fig. 10 and Fig. 11.

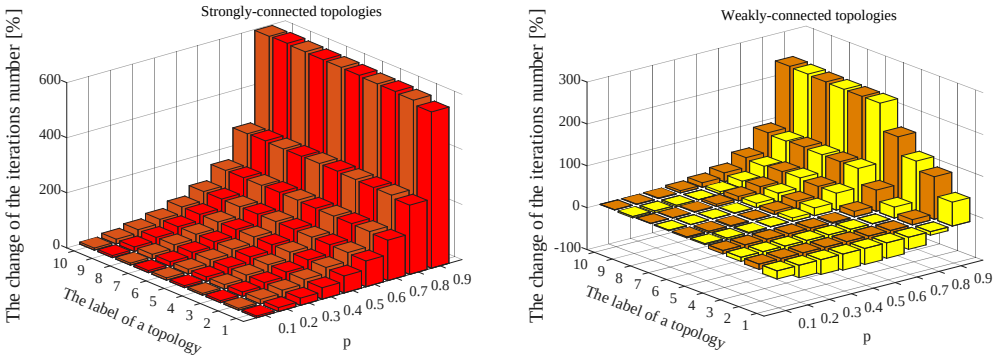

Fig. 10. The impact of a links failure on the change of the number of the iterations

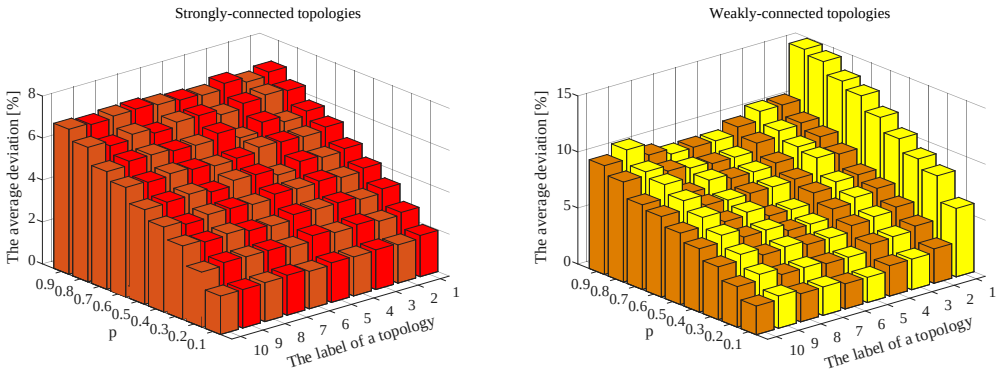

Fig. 11. The impact of a links failure on the deviation of the final results from the expected ones

We can see from the results that for higher values of p, both parameters achieve worse results than for smaller values. In the strongly–connected ones, a links failure causes a more significant deceleration of the computation process, meanwhile, in the weakly–connected networks, this failure has a more massive impact on the precision of the final results. In the weakly–connected structures, we can also see interesting phenomenon – a links failure can accelerate the computation process. The change of the iterations number has also a specific character in these networks – the number of the iterations decreases, then reaches the maximal acceleration and begins to grow. Also, we can see that the behavior of the examined parameters within the same set is much more similar in strongly–connected ones.

3 Conclusion

In this paper, we examine the impact of a links failure on the push–sum protocol calculating the average. We assume two types of networks: strongly and weakly–connected. In the first section, we focus our attention on a verification of the mass conservation theorems, which ensure a proper functionality of the push–sum protocol. Regardless of the probability of a link failure, the mentioned theorems are not preserved due to lost messages and therefore, the push–sum protocol is unable

to execute the mistake–free calculation of the average. A higher value of *p* results in a higher deviation of both the sums from the expected values. In the next section, we examine the impact on the distribution of the convergences rates. We can observe that in the strongly connected structures, a higher value of *p* decelerates the protocol as well as causes a higher variance of the obtained data. Meanwhile, in the weakly–connected structures, we observe the interesting phenomenon – failures of the links may accelerate the whole computation process. This happens for smaller values of *p*. In the third section, we examine the impact of a links failure on the diversity of the final results to which the nodes convergence. In both types of the networks, higher values of *p* cause a higher diversity. In general, a higher diversity is more significantly observed in the weakly–connected structures. In the last experiment, we examine the change of the convergence rates and the deviation of the final values to which the nodes convergence from the expected ones. We can see that the first parameter achieves better results in the weakly–connected structures, meanwhile, the other one is smaller in strongly–connected structures.

Acknowledgements. Research described in this paper was financed by the National Sustainability Program under grant LO1401. For the research, infrastructure of the SIX Center was used.

References

[1] D. Kempe, A. Dobra and J. Gehrke, Gossip-based computation of aggregate information, *Foundations of Computer Science, 2003. Proceedings. 44th Annual IEEE Symposium on,* (2003), 482-491. http://dx.doi.org/10.1109/sfcs.2003.1238221

[2] J. Kenyeres, M. Kenyeres, M. Rupp, P. Farkaš, Connectivity-Based Self-Localization in WSNs, *Radioengineering,* **22** (2013), no. 3, 818-827.

[3] P. Lopez Iturri, L. Azpilicueta, J.A. Nazabal, C. Fernandez-Valdivielso, J. Soret, F. Falcone, Analysis of energy consumption performance towards optimal radioplanning of wireless sensor networks in heterogeneous indoor environments, *Radioengineering,* **23** (2014), no. 3, 852–862.

[4] B.K. Mandal, D. Bhattacharyya and K.H. Shim, A Security Architecture for Wireless Sensor Network Environmental, *Contemporary Engineering Sciences,* **7** (2014), no. 15, 737-742. http://dx.doi.org/10.12988/ces.2014.4683

[5] M. Mousazadeh and B.T. Ladani, Gossip-based data aggregation in hostile environment, *Computer Communications,* **62** (2015), 1-12. http://dx.doi.org/10.1016/j.comcom.2015.02.002

Received: July 5, 2016; Published: September 14, 2016